

CARLOS MARÍA ROMEO CASABONA
M.^a ÁNGELES RUEDA MARTÍN
Editores

DERECHO PENAL, CIBERSEGURIDAD,
CIBERDELITOS E INTELIGENCIA ARTIFICIAL

VOLUMEN I
CIBERSEGURIDAD Y CIBERDELITOS

GRANADA, 2023

BIBLIOTECA COMARES DE CIENCIA JURÍDICA

**ESTUDIOS DE DERECHO PENAL
Y CRIMINOLOGÍA**

dirigidos por

Carlos María Romeo Casabona

143

© Los autores

Editorial Comares, 2023

Polígono Juncaril

C/ Baza, parcela 208

18220 Albolote (Granada)

Tif.: 958 465 382

<http://www.editorialcomares.com> • E-mail: libreriacomares@comares.com

<https://www.facebook.com/Comares> • <https://twitter.com/comareseditor>

<https://www.instagram.com/editorialcomares>

ISBN: 978-84-1369-670-6 • Depósito legal: 1646/2023

Fotocomposición, impresión y encuadernación: Comares

SUMARIO

ABREVIATURAS	XIX
PRESENTACIÓN	XXI

PRIMERA PARTE

EL CIBERESPACIO Y LA CIBERSEGURIDAD COMO NUEVO MARCO PARA LA CIBERDELINCUENCIA

CAPÍTULO I

EL CIBERESPACIO COMO LUGAR VIRTUAL Y LEGAL DE COMISIÓN DEL DELITO. NECESIDADES DE NUEVAS RESPUESTAS JURÍDICAS

CARLOS MARÍA ROMEO CASABONA

I. EL CIBERESPACIO COMO <i>LOCUS DELICTI COMMISSI</i> VIRTUAL	3
1. Acotación conceptual	3
2. Ciberespacio y soberanía estatal: su extraterritorialidad	5
II. AGRESIONES EN EL CIBERESPACIO: LOS CIBERATAQUES	5
1. Los ciberataques, manifestación de las formas actuales de los ciberdelitos	5
2. La vulnerabilidad del ciberespacio	6
III. LA CIBERSEGURIDAD: UN CONCEPTO DIFUSO EN EXPANSIÓN Y UN FENÓMENO NECESITADO DE UN MARCO LEGAL AMPLIO	7
IV. LOS CIBERDELITOS: SU EVOLUCIÓN POLÍTICO-CRIMINAL	10
1. La construcción del futuro Derecho Penal de las tecnologías de la información y la comunicación	10
2. ¿Situaciones conflictivas para el futuro? El caso de los vehículos de transporte inte- ligentes	11
V. LA CIBERGUERRA Y LA CIBERDEFENSA	14
1. Aproximación conceptual a la ciberguerra, a la ciberdefensa y otros comportamientos próximos	14

1.1. <i>La ciberguerra y la ciberdefensa</i>	14
1.2. <i>Conflictos híbridos</i>	17
1.3. <i>El ciberterrorismo como una forma diferente de ciberataque o ciberguerra</i> . . .	17
1.4. <i>Otros ciberataques contra intereses públicos</i>	17
2. El Estado como víctima de los ciberataques. La ciberdefensa legal.	18
3. Otros aspectos generales de la ciberdefensa.	18
VI. COOPERACIÓN INTERNACIONAL	18
BIBLIOGRAFÍA	20

CAPÍTULO 2

AMENAZAS COMPLEJAS EN EL CIBERESPACIO,
ESTADO DEL ARTE Y PROSPECTIVA

LUIS FERNANDO HERNÁNDEZ GARCÍA

I. INTRODUCCIÓN	23
II. ANÁLISIS DE LAS CIBERAMENAZAS ACTUALES	26
1. Seguridad, término antiguo, concepto nuevo	28
2. Ciberseguridad, la seguridad en el Ciberespacio	32
3. Ciberamenazas, las nuevas amenazas transnacionales.	37
3.1. <i>El ciberdelito / Cibercrimen / Delito informático</i>	51
3.2. <i>Ciberterrorismo</i>	54
3.3. <i>Hactivismo / Ciberyihadismo</i>	73
3.4. <i>Ciberespionaje</i>	78
3.5. <i>Ciberguerra</i>	82
III. PROSPECTIVA	87

CAPÍTULO 3

EL CIBERESPACIO COMO NUEVO ESCENARIO PARA VULNERAR
DERECHOS FUNDAMENTALES

AITZIBER EMALDI CIRIÓN

I. INTRODUCCIÓN Y ESTADO DE LA CUESTIÓN	101
II. EL CIBERESPACIO Y LA CIBERSEGURIDAD	102
1. El ciberespacio.	102
2. La ciberseguridad.	103
III. DEBILIDADES DEL CIBERESPACIO	106
IV. AMENAZAS FRENTE A LAS DEBILIDADES DEL CIBERESPACIO Y MEDIDAS DE ACTUACIÓN	107
1. Atacantes del ciberespacio.	108
2. Medidas de actuación de los poderes públicos.	110
V. DERECHOS CONSTITUCIONALES VULNERADOS POR EL CIBERCRIMEN	111
1. La dignidad de la persona y el libre desarrollo de la personalidad.	112
2. Derecho a la no discriminación	114

3. El derecho al honor, a la intimidad y a la propia imagen en relación con el derecho a la protección de datos	116
4. Derechos de los consumidores	119
5. Derecho a la seguridad ciudadana	122
VI. CONCLUSIONES	123
BIBLIOGRAFÍA	125

CAPÍTULO 4

LA INTROMISIÓN DEL DERECHO PENAL EN LA PROTECCIÓN
DE LA CIBERSEGURIDAD

ESTEBAN SOLA RECHE

I. INTRODUCCIÓN	127
1. El cambiante objeto de protección penal y la ciberseguridad.	127
2. Preferencia por el concepto «tecnologías de la comunicación» frente al de «tecnologías de la información» como instrumento del delito.	130
II. SENTIDO, CONTENIDOS Y CONCEPTO (JURÍDICAMENTE MANEJABLE) DE CIBERSEGURIDAD	131
1. La seguridad como bien jurídico	133
2. Manifestación cibernética de la seguridad (ciberseguridad).	134
3. La ciberseguridad como objeto de protección por el Derecho penal	136
IV. CONCLUSIONES SOBRE LAS PREVISIONES	138

CAPÍTULO 5

ALGUNAS REFLEXIONES JURÍDICAS SOBRE LOS DELITOS DEL SIGLO XXI:
CIBERCRIMEN, INTERNET OSCURA Y Covid-19

ELENA ATIENZA MACÍAS

SILVIA IRENE VERDUGO GUZMÁN

I. DELITOS DEL SIGLO XXI. LA CIBERDELINCUENCIA	143
II. CIBERESPACIO, INTERNET SUPERFICIAL Y DARKNET.	145
1. Regulación normativa transfronteriza	147
2. Los delitos digitales en España	148
3. Cibercrimen del entorno digital	149
4. Estafas informáticas y secuestro de información digital a causa del Covid-19	150
5. Rescates de la información mediante criptomonedas. Los Bitcoins.	152
III. INTELIGENCIA ARTIFICIAL Y TRANSFORMACIÓN DIGITAL	153
1. Conceptos generales de I.A	153
2. La I.A. frente al cibercrimen	154
IV. CONCLUSIONES	157
BIBLIOGRAFÍA	158

CAPÍTULO 6

EL PROTOCOLO ADICIONAL AL CONVENIO SOBRE CIBERDELINCUENCIA
COMO RESPUESTA INTEGRADORA ANTE LAS DIFICULTADES
EN LA ATRIBUCIÓN DE LA JURISDICCIÓN PENAL

EKAIN PAYÁN ELLACURIA

I. INTRODUCCIÓN	161
II. VIGENCIA ESPACIAL DE LA LEY PENAL	164
1. Principio de territorialidad	164
2. Principios de ultraterritorialidad	165
2.1. <i>Personalidad</i>	165
2.2. <i>Real o de protección de intereses</i>	166
2.3. <i>Justicia universal</i>	166
III. EL LUGAR DE COMISIÓN DE LOS DELITOS CONEXOS INTERNACIONALES	167
1. Teorías de la actividad, del resultado y de la ubicuidad	168
2. Los conflictos de jurisdicción a la luz de la jurisprudencia internacional	170
IV. LA JURISDICCIÓN PENAL EN EL CONVENIO DE BUDAPEST Y ALGUNAS RESPUESTAS JURÍDICAS PARA SU ARMONIZACIÓN	175
V. CONSIDERACIONES FINALES	179
BIBLIOGRAFÍA	182

SEGUNDA PARTE

LOS CIBERDELITOS EN EL CÓDIGO PENAL ESPAÑOL

CAPÍTULO 7

LA RESPUESTA DEL DERECHO PENAL ESPAÑOL ANTE LOS ATAQUES
CONTRA LOS SISTEMAS DE INFORMACIÓN. UN ANÁLISIS CRÍTICO

ALIUSKA DUARDO SÁNCHEZ

I. INTRODUCCIÓN	189
1. Contexto	189
2. Ataques a los sistemas de información. Una aproximación conceptual	190
II. LA POLÍTICA CRIMINAL EUROPEA ANTE LOS CIBERATAQUES	193
1. El convenio de Budapest	193
2. Política criminal de la Unión Europea	196
2.1. <i>La Directiva sobre ataques a sistemas de información</i>	196
2.2. <i>El Reglamento (UE) 2019/796: medidas restrictivas contra los ciberataques que amenacen a la UE o a sus Estados miembros</i>	198
III. LA RESPUESTA DEL DERECHO PENAL ESPAÑOL	201
IV. CONCLUSIONES	206
BIBLIOGRAFÍA	208

CAPÍTULO 8
ANÁLISIS JURISPRUDENCIAL DE LOS DELITOS CONTRA DATOS RESERVADOS
DESDE LA PERSPECTIVA DE LA CIBERSEGURIDAD

CARLOS TRINCADO CASTÁN

I.	INTRODUCCIÓN	209
II.	ARTÍCULO 197: DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS Y DATOS DE CARÁCTER PERSONAL Y FAMILIAR	212
	1. El solapamiento de los apartados 1 y 2 del artículo 197 CP cuando los secretos están almacenados en registros y ficheros informáticos	212
	2. Artículo 197, apartado 2 del CP. La diferencia entre el inciso primero y el inciso segundo: implicaciones desde el punto de vista de la ciberseguridad	214
	3. Artículo 197.2 CP: accesos por intraneí. La relevancia de las políticas de uso de sistemas informáticos	216
	4. Artículo 197.2 CP: accesos por extraneí	221
	5. La vulneración de medidas de seguridad en el artículo 197.2 CP.	225
II.	ARTÍCULO 200: DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS DE PERSONAS JURÍDICAS.	226
	1. La Conducta típica: descubrir, revelar o ceder datos reservados de personas jurídicas sin el consentimiento de sus representantes	227
	2. Concepto de datos reservados de persona jurídica	228
	3. Sujetos activos	231
III.	ARTÍCULO 278: APODERAMIENTO Y REVELACIÓN DE SECRETOS DE EMPRESA	232
	1. El concepto de secretos de empresa	233
	2. Apoderarse por cualquier medio de datos, documentos, soportes informáticos u otros objetos y difundirlos, revelarlos o cederlos	236
	3. Sujetos activos	237
IV.	CONCLUSIONES	239
	BIBLIOGRAFÍA	240

CAPÍTULO 9
EL DELITO DE INTRUSIÓN EN UN SISTEMA DE INFORMACIÓN

CARLOS MARÍA ROMEO CASABONA

I.	ASPECTOS GENERALES Y POLÍTICO-CRIMINALES	241
	1. Configuración y evolución del delito	241
	2. El delito de intrusión en la normativa europea e interna	242
	3. Aspectos de política criminal.	243
II.	EL BIEN JURÍDICO PROTEGIDO Y EL OBJETO MATERIAL DEL DELITO.	246
	1. El bien jurídico protegido.	246
	2. El objeto material del delito.	248
III.	MODALIDADES TÍPICAS	248
	1. Acceder a un sistema de información o mantenerse en él vulnerando las medidas de seguridad establecidas	249
	1.1. <i>El tipo objetivo</i>	249
	1.2. <i>El tipo subjetivo</i>	251

XIV	DERECHO PENAL, CIBERSEGURIDAD, CIBERDELITOS E INTELIGENCIA ARTIFICIAL, VOL. I	
	2. Interceptación de transmisiones no públicas de datos informáticos	251
IV.	ACTOS PREPARATORIOS RELATIVOS AL DELITO DE INTRUSIÓN EN UN SISTEMA DE INFORMACIÓN	252
V.	COMISIÓN DE LA INTRUSIÓN POR ORGANIZACIÓN O GRUPO CRIMINAL Y POR PERSONAS JURÍDICAS	253
VI.	PROPUESTAS DE <i>LEGE FERENDA</i> . ¿LA (CIBER)SEGURIDAD COMO BIEN JURÍDICO?	254
	BIBLIOGRAFÍA	257

CAPÍTULO 10
EL DELITO DE DAÑOS INFORMÁTICOS ANTE NUEVOS
ESCENARIOS TECNOLÓGICOS

PILAR NICOLÁS

I.	EL ENTORNO DIGITAL COMO MEDIO EN EL QUE SE DESENVUELVE LA VIDA DEL SIGLO XXI. . .	259
II.	ANTECEDENTES Y EVOLUCIÓN DEL DELITO DE DAÑOS INFORMÁTICOS	261
III.	DATOS INFORMÁTICOS, PROGRAMAS INFORMÁTICOS O DOCUMENTOS ELECTRÓNICOS AJENOS . . .	263
IV.	LOS RECURSOS QUE GARANTIZAN EL FUNCIONAMIENTO DEL ENTORNO DIGITAL COMO BIEN JURÍDICO PROTEGIDO.	265
V.	LA GRAVEDAD EN EL DELITO DE DAÑOS INFORMÁTICOS.	268
	1. Gravedad de la conducta y gravedad del resultado.	268
	2. Las agravaciones	271
VI.	CONCLUSIONES	272

CAPÍTULO 11
LOS ATAQUES DE DENEGACIÓN DE SERVICIOS
COMO CIBERDELITO EN EL CÓDIGO PENAL ESPAÑOL

M.^a ÁNGELES RUEDA MARTÍN

I.	INTRODUCCIÓN.	275
II.	LOS ATAQUES DE DENEGACIÓN DE SERVICIOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL ÁMBITO INTERNACIONAL Y DE LA UNIÓN EUROPEA: PROPUESTA POLÍTICO CRIMINAL	280
III.	EL BIEN JURÍDICO PROTEGIDO EN EL DELITO DE DENEGACIÓN DE SERVICIOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN. REFLEXIONES SOBRE SU PROTECCIÓN PENAL	281
IV.	OPCIONES POLÍTICO CRIMINALES PARA TIPIFICAR LOS ATAQUES DE DENEGACIÓN DE SERVICIOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN.	301
V.	EL TIPO BÁSICO DEL DELITO DE DENEGACIÓN DE SERVICIOS DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN	307
VI.	AGRAVACIONES ESPECÍFICAS.	313
	1. La obstaculización o interrupción del funcionamiento de un sistema informático ajeno de una manera grave en el marco de una organización criminal	314
	2. Daños de especial gravedad, afectación a un elevado número de sistemas informáticos o un perjuicio grave al funcionamiento de servicios públicos esenciales o a la provisión de bienes de primera necesidad	316

3. Afectación al sistema de información de una infraestructura crítica o creación de un peligro grave para la seguridad del Estado, de la Unión Europea o de un Estado miembro de la Unión Europea	317
4. Comisión del hecho por la utilización de determinados instrumentos	318
5. Hechos de extrema gravedad	319
6. La obstaculización o interrupción de un sistema informático ajeno de una manera grave mediante la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero	319
VII. ACTOS PREPARATORIOS PUNIBLES	320
VIII. LA RESPONSABILIDAD PENAL DE LAS PERSONAS JURÍDICAS	322
IX. REFLEXIONES EN TORNO A LA DETERMINACIÓN DE LA LEY PENAL APLICABLE EN LOS ATAQUES DE DENEGACIÓN DE SERVICIOS TRANSFRONTERIZOS	323
X. LA PENALIZACIÓN DE LOS ATAQUES DE DENEGACIÓN DE SERVICIOS COMO CIBERDELITO EN EL CÓDIGO PENAL ESPAÑOL, ¿OFRECE UNA RESPUESTA ADECUADA FRENTE A LAS AMENAZAS Y ATAQUES QUE SE CIERNEN SOBRE LA CIBERSEGURIDAD?	324

CAPÍTULO 12

¿SON LOS ACTOS PREPARATORIOS DE LOS ARTÍCULOS 197 TER
Y 264 TER DEL CÓDIGO PENAL RESULTADO DE UNA INADECUADA
ADAPTACIÓN DE LA NORMATIVA PENAL COMUNITARIA E INTERNACIONAL? UNA
PROPUESTA DE *LEGE FERENDA*

IKER CONAL FUERTES

I. LOS ARTÍCULOS 197 TER Y 264 TER DEL CÓDIGO PENAL ESPAÑOL	327
1. Introducción.	327
2. Contenido.	328
2.1. <i>Artículo 197 ter</i>	330
2.2. <i>Artículo 264 ter</i>	332
II. PROBLEMÁTICA QUE PLANTEAN	332
1. Los solapamientos	332
2. Su incorrecta identificación como actos preparatorios	334
III. ¿UNA ADAPTACIÓN INADECUADA?	341
1. Las adaptaciones alternativas realizadas en el Derecho comparado.	341
1.1. <i>Alemania</i>	341
1.2. <i>Reino Unido</i>	342
2. La esencial distinción entre contenido obligatorio y voluntario.	343
2.1. <i>En la ejecución del Derecho penal internacional</i>	343
2.2. <i>En la transposición del Derecho penal comunitario</i>	344
3. Los errores técnicos de los que adolece la adaptación	345
IV. UNA PROPUESTA DE <i>LEGE FERENDA</i> ORIENTADA A HACER FRENTE A LOS ATAQUES CONTRA LA CIBERSEGURIDAD DE MANERA EFICAZ.	347
V. CONCLUSIONES	350
BIBLIOGRAFÍA	351

CAPÍTULO 13
LA APLICACIÓN DE LOS DELITOS CONTRA LOS SISTEMAS
DE INFORMACIÓN POR LOS TRIBUNALES ESPAÑOLES

CARLOS TRINCADO CASTÁN

I.	INTRODUCCIÓN	353
II.	ARTÍCULO 197 BIS: ACCESOS ILÍCITOS A SISTEMAS INFORMÁTICOS	357
	1. El delito de intrusión ilícita a sistemas informáticos: Casuística	358
	1.1. <i>Audiencias provinciales, casuística: empresas</i>	359
	1.2. <i>Audiencias provinciales, casuística: universidades</i>	359
	1.3. <i>Audiencias provinciales, casuística: accesos a redes sociales</i>	360
	2. El debate sobre el bien jurídico protegido en el artículo 197 bis	360
	3. El concepto de acceso no autorizado a sistemas informáticos	365
	4. Vulneración de medidas de seguridad	367
	5. La problemática diferenciación de los delitos de los artículos 197.2 y 197 bis CP	370
	6. El ámbito de aplicación del tipo agravado del artículo 198 CP	372
III.	ARTÍCULO 264 BIS CP: LA INTERRUPCIÓN Y OBSTACULIZACIÓN DE SISTEMAS INFORMÁTICOS	373
	1. Aplicación del artículo 264 bis CP tras la reforma de 2015	374
	2. Interrupciones de sistemas informáticos anteriores a la reforma de 2015	378
	2.1. <i>Interrupción de sistema informático mediante virus ransomware</i>	378
	2.2. <i>Interrupción de sistemas informáticos mediante ataques DDoS (Denegación de Servicio Distribuida)</i>	379
	2.3. <i>Otros casos</i>	380
	3. Los tipos agravados del 264 bis	382
	4. Bien jurídico y concursos de delitos.	386
	5. El delito del artículo 264 ter a) CP.	388
IV.	CONCLUSIONES	389
	BIBLIOGRAFÍA	390

CAPÍTULO 14
RESPUESTA PENAL A LA SUPLANTACIÓN DE IDENTIDAD.
ESPECIAL CONSIDERACIÓN A LOS FRAUDES DE IDENTIDAD DIGITAL

FÁTIMA FLORES MENDOZA

I.	APROXIMACIÓN A LA SUPLANTACIÓN DE IDENTIDAD	395
II.	RESPUESTA PENAL A LA SUPLANTACIÓN DE IDENTIDAD.	402
	1. A través del delito de usurpación del estado civil (art. 401 CP).	404
	2. A través de los delitos de falsedad documental (art. 390 y ss. CP).	408
	3. A través de los diversos delitos cometidos mediante suplantación de identidad	411
	4. A través de los delitos que castigan el denominado hurto de identidad	416
	5. ¿A través de un nuevo delito? Sobre la necesidad político-criminal de tipificar los fraudes de identidad.	417

CAPÍTULO 15
LA PROPORCIONALIDAD DE LA RESPUESTA PENAL
AL CIBERESPIONAJE INDUSTRIAL Y AL DESCUBRIMIENTO
Y REVELACIÓN DE SECRETOS POR MEDIO DE LA RED

EMILIO JOSÉ ARMAZA ARMAZA

JON LÓPEZ GOROSTIDI

I.	PLANTEAMIENTO DEL PROBLEMA Y OBJETIVOS DE LA CONTRIBUCIÓN	423
II.	LA POTENCIAL MAYOR CAPACIDAD LESIVA DE LAS CONDUCTAS CIBERINTRUSIVAS	424
	1. La lógica del funcionamiento de la red y de las TIC	424
	2. El perfil del sujeto activo en los delitos de ciberespionaje	426
	3. La permanencia del hecho en la red y la pluralidad de víctimas	427
	4. La contracción del ciberespacio	428
	5. La relatividad temporal de los ciberdelitos	429
	6. La facilidad de encubrimiento y la dificultad de persecución de la ciberdelin- cuencia	430
III.	UNA HERRAMIENTA PARA LA MEDICIÓN DE LA PROPORCIONALIDAD: LA FÓRMULA DEL PESO DE ALEXY	432
IV.	EXAMEN DE LA PROPORCIONALIDAD EN LOS DELITOS DE CIBERESPIONAJE	439
	1. Análisis de la proporcionalidad en el delito de espionaje industrial	440
	2. Análisis de la proporcionalidad en el delito de descubrimiento y revelación de secretos	445
V.	CONCLUSIONES	449
BIBLIOGRAFÍA		451

CAPÍTULO 16
LA RESPUESTA JURÍDICA DEL CÓDIGO PENAL ESPAÑOL A LOS CIBERDELITOS
COMETIDOS EN EL ÁMBITO DE ORGANIZACIONES O GRUPOS CRIMINALES

MIGUEL ÁNGEL BOLDOVA PASAMAR

I.	INTRODUCCIÓN	453
II.	CIBERDELITOS EN SENTIDO AMPLIO Y PREVISIÓN, EN SU CASO, DE TIPOS CUALIFICADOS POR ORGANIZACIÓN O GRUPO CRIMINAL	454
III.	EL CRIMEN ORGANIZADO COMO DELITO AUTÓNOMO	459
IV.	LOS TIPOS CUALIFICADOS DE PERTENENCIA A ORGANIZACIÓN O GRUPO CRIMINAL: INTER- PRETACIÓN TELEOLÓGICO-RESTRICTIVA	467
V.	LA PROBLEMÁTICA CONCURSAL	471
VI.	REFERENCIA ESPECÍFICA A ORGANIZACIONES Y GRUPOS TERRORISTAS	476
VII.	CONCLUSIONES Y PROPUESTAS DE <i>LEGE FERENDA</i>	478

LOS AUTORES DE LA OBRA

A.	MIEMBROS Y PARTICIPANTES EN EL PROYECTO DE INVESTIGACIÓN	481
B.	COAUTORES INVITADOS AJENOS AL PROYECTO	482

CARLOS MARÍA ROMEO CASABONA
M.^a ÁNGELES RUEDA MARTÍN
Editores

DERECHO PENAL, CIBERSEGURIDAD,
CIBERDELITOS E INTELIGENCIA ARTIFICIAL

VOLUMEN II
INTELIGENCIA ARTIFICIAL Y RESPONSABILIDAD PENAL

BIBLIOTECA COMARES DE CIENCIA JURÍDICA

**ESTUDIOS DE DERECHO PENAL
Y CRIMINOLOGÍA**

dirigidos por

Carlos María Romeo Casabona

144

© Los autores

Editorial Comares, 2023

Polígono Juncaril

C/ Baza, parcela 208

18220 Albolote (Granada)

Tlf.: 958 465 382

<http://www.editorialcomares.com> • E-mail: libreriacomares@comares.com

<https://www.facebook.com/Comares> • <https://twitter.com/comareseditor>

<https://www.instagram.com/editorialcomares>

ISBN: 978-84-1369-671-3 • Depósito legal: 1647/2023

Fotocomposición, impresión y encuadernación: Comares

SUMARIO

ABREVIATURAS	XIII
--------------------	------

TERCERA PARTE

EN LA FRONTERA DE LOS CIBERDELITOS Y LA IA: LIBERTAD DE EXPRESIÓN, DATOS PERSONALES Y EL BIG DATA

CAPÍTULO 17

LA PROTECCIÓN DE DATOS PERSONALES EN LA UNIÓN EUROPEA. ASPECTOS SECTORIALES RELACIONADOS CON LA SALUD

CARLOS MARÍA ROMEO CASABONA

I. EL FLUJO NORMATIVO RELATIVO A LOS DATOS Y EL DESARROLLO DE UN MARCO GENERAL PARA SU PROTECCIÓN.	3
II. LA OBTENCIÓN DE GRANDES VOLÚMENES DE INFORMACIÓN RELACIONADA CON LA SALUD, HERRAMIENTA ESENCIAL DE LA MPP. EL BIG DATA	6
III. EL TRATAMIENTO DE LOS DATOS DE SALUD MASIVOS RECOGIDOS A LO LARGO DE LA VIDA DE UNA PERSONA	8
1. Nuevas formas de manifestación de los datos	9
1.1. <i>Los riesgos de reidentificación: la insuficiencia de los procedimientos de anonimización de los datos. La seudonimización</i>	10
1.2. <i>Prevención del automatismo en la toma de decisiones asistenciales.</i>	13
1.3. <i>Elaboración de perfiles de los pacientes</i>	14
2. La protección jurídica reforzada de los datos de salud y su extensión a datos con relevancia para la salud	14
3. El Delegado de Protección de Datos	15
IV. LA GESTIÓN DE GRAN VOLUMEN DE INFORMACIÓN SENSIBLE Y LA UTILIZACIÓN DE HERRAMIENTAS «BIG DATA» EN LA ASISTENCIA CLÍNICA O EN MODELOS PREDICTIVOS	16

VIII	DERECHO PENAL, CIBERSEGURIDAD, CIBERDELITOS E INTELIGENCIA ARTIFICIAL, VOL. II	
V.	RETOS ABIERTOS PARA LA PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES RELATIVOS A LA SALUD	19
VI.	NUEVAS PERSPECTIVAS PARA EL EJERCICIO DE LA AUTONOMÍA POR LOS PACIENTES.	22
VII.	COMERCIALIZACIÓN DE LOS DATOS DE SALUD PERSONALES.	23
	BIBLIOGRAFÍA	26

CAPÍTULO 18

LA DESINFORMACIÓN EN EL CIBERESPACIO: LAS NOTICIAS FALSAS
Y SU PERSECUCIÓN PENAL

CARLOS MARÍA ROMEO CASABONA

I.	LA DESINFORMACIÓN, UN CONCEPTO CONFUSO	29
II.	LA SOBREENFORMACIÓN COMO CONTEXTO PROPICIADOR DE LA DESINFORMACIÓN.	31
III.	NOTICIAS FALSAS, DESINFORMACIÓN Y DERECHOS FUNDAMENTALES	32
IV.	LA EXPANSIÓN DE LA DESINFORMACIÓN Y DE LAS NOTICIAS FALSAS RELACIONADAS CON LA PANDEMIA DEL VIRUS SARS-COV-2	36
V.	LA INTERVENCIÓN DEL DERECHO PENAL ANTE LAS NOTICIAS FALSAS.	38
	1. ¿Límites generales a la difusión de contenidos en las redes? ¿Censura previa?	38
	2. Las respuestas del Derecho Penal de lege lata contra las noticias falsas	42
VI.	LÍMITES DE LOS DELITOS: LA ANTIJURICIDAD. LA COLISIÓN CON LAS LIBERTADES DE EXPRESIÓN Y DE INFORMACIÓN	45
VII.	¿PROPUESTAS DE <i>LEGE FERENDA</i> ?	47
VIII.	RESPUESTAS NO PENALES CONTRA LAS NOTICIAS FALSAS	49
IX.	CONSIDERACIONES FINALES	51
	BIBLIOGRAFÍA	52

CUARTA PARTE

INTELIGENCIA ARTIFICIAL Y ATRIBUCIÓN
DE RESPONSABILIDAD PENAL

CAPÍTULO 19

LA DISCUSIÓN SOBRE LA ATRIBUCIÓN DE RESPONSABILIDAD
PENAL A SISTEMAS DE INTELIGENCIA ARTIFICIAL,
EN PARTICULAR A SISTEMAS AUTÓNOMOS

CARLOS MARÍA ROMEO CASABONA

I.	INTRODUCCIÓN	57
II.	¿NECESITAMOS UN NUEVO SISTEMA PENAL CONSTRUIDO PARA LA IA Y LOS ROBOTS?	60
III.	¿VALIDEZ DE LOS ESTÁNDARES LEGALES PARA RESOLVER PROBLEMAS DE RESPONSABILIDAD DE SISTEMAS DE IA POR DAÑOS A PERSONAS O COSAS? RESPONSABILIDAD PENAL POR IMPRUDENCIA	62
IV.	LESIONES DE BIENES JURÍDICOS PRODUCIDAS INTENCIONADAMENTE	67

1. El robot o el sistema de IA, como meros instrumentos de la acción humana	67
2. Sistemas autónomos inteligentes: ¿agentes criminales?	68
V. ASPECTOS ESPECÍFICOS RELATIVOS A LA RESPONSABILIDAD PENAL DE SISTEMAS AUTÓNOMOS INTELIGENTES	70
1. Argumentos a favor de atribuir responsabilidad penal a los robots, sistemas inteligentes y tecnologías conexas autónomas	71
2. Argumentos contrarios a la criminalización directa de los sistemas de IA	74
VI. LA ATRIBUCIÓN DE RESPONSABILIDAD PENAL A LOS ROBOTS AUTÓNOMOS Y A LOS SISTEMAS INTELIGENTES: EL CONTROL HUMANO DE LOS SISTEMAS DE IA COMO ENFOQUE ALTERNATIVO PREVIO	76
VII. MIRANDO AL FUTURO	79
BIBLIOGRAFÍA	80

CAPÍTULO 20

LA «INTELIGENCIA ARTIFICIAL» EN LA JUSTICIA PENAL
ANTE EL PRINCIPIO DE RESPONSABILIDAD PERSONAL

ANDREA PERIN

I. INTRODUCCIÓN	83
II. PARADIGMAS DE «INTELIGENCIA ARTIFICIAL»	84
III. IA Y RESPONSABILIDAD PERSONAL	85
1. La «agencia moral»	86
2. Autonomía y «autoconsciencia sintiente» en los humanos responsables	90
3. Medidas de seguridad para los agentes artificiales	92
IV. LA IA COMO INSTRUMENTO DE LA JUSTICIA PENAL	95
1. Modelos y empleos	95
2. La justicia penal «predictiva» y sus límites: previsión vs. juicio y decisión	95
3. Imputación de responsabilidad (juicio) vs. pronóstico de peligrosidad (previsión)	98
3.1. <i>Neurobiología de la voluntad e imputación de responsabilidad individual: compatibilidad.</i>	99
3.2. <i>Neurobiología de la voluntad y pronóstico de peligrosidad: probabilidad.</i>	100
4. Aplicación de penas (decisión) y pronóstico de peligrosidad (previsión): solapamientos entre penas y medidas de seguridad	101
5. Decidir sin juzgar: las ideologías de la «justicia predictiva»	103
6. Límites funcionales de la previsión algorítmica ante la configuración de la justicia penal	104
6.1. <i>Seguridad y precisión (fiabilidad)</i>	105
6.2. <i>Neutralidad (ausencia de sesgos cognitivos y prejuicios culturales).</i>	106
6.3. <i>Eficiencia vs. evolución liberal del derecho penal.</i>	111
V. SÍNTESIS Y PERSPECTIVAS	112
BIBLIOGRAFÍA	115

CAPÍTULO 21
INTELIGENCIA ARTIFICIAL, PREDICTIVIDAD Y JUSTICIA PENAL

CARLOS MARÍA ROMEO CASABONA

I.	PLANTEAMIENTO	119
II.	EL MÉTODO ACTUARIAL MEDIANTE LA UTILIZACIÓN AUTOMATIZADA DE ALGORITMOS.	121
III.	EL MÉTODO ACTUARIAL SUSTENTADO EN EL PROCESAMIENTO AUTOMATIZADO DE ALGORITMOS PARA PREDECIR EL RIESGO DE RECIDIVA CRIMINAL: PRIMERAS SENTENCIAS EN DERECHO COMPARADO	122
IV.	EL TRATAMIENTO AUTOMATIZADO DE DATOS EN EL DERECHO EUROPEO	132
V.	CONSIDERACIONES FINALES	135
BIBLIOGRAFÍA		138

CAPÍTULO 22

LA PROPUESTA DE REGLAMENTO «LEY DE INTELIGENCIA ARTIFICIAL»:
ANÁLISIS DE SU POSIBLE IMPACTO EN LA UTILIZACIÓN DE SISTEMAS
AUTOMATIZADOS EN EL ÁMBITO DEL DERECHO PENAL

GUILLERMO LAZCOZ MORATINOS

ASIER URRUELA MORA

IÑIGO DE MIGUEL BERIAIN

I.	INTRODUCCIÓN: LA UE TRAS LA REGULACIÓN DE LA IA	141
II.	PROPUESTA DE REGLAMENTO «LEY DE INTELIGENCIA ARTIFICIAL»	142
	1. Sistemas de IA de alto riesgo: Aplicación de la propuesta en el ámbito del Derecho penal y de la ciberseguridad.	145
	1.1. <i>Problemática de los sesgos vinculados al empleo de las herramientas fundadas en la IA en la determinación de la peligrosidad criminal (ámbito penal)</i>	149
	1.1.1. <i>Tratamiento de los sesgos vinculados a la IA en el informe del Panel para el Futuro de la Ciencia y la Tecnología (STOA)</i>	151
	1.1.2. <i>La toma en consideración de los sesgos de la IA en la Propuesta de Reglamento «Ley de inteligencia artificial». Perspectiva crítica a partir del Dictamen conjunto 5/2021 del Comité Europeo de Protección de datos (CEPD) y del Supervisor Europeo de Protección de Datos (SEPD)</i>	153
	1.2. <i>Supervisión humana como requisito obligatorio</i>	155
III.	POSIBLE IMPACTO DE LA PROPUESTA EN EL PROCESO PENAL A PARTIR DE CASOS DE USO REALES	158
	1. VioGén.	159
	2. COMPAS	161
IV.	CONCLUSIONES	163

QUINTA PARTE
INFORME Y CONCLUSIONES

Capítulo 23

CIBERSEGURIDAD, CIBERDELITOS E INTELIGENCIA ARTIFICIAL:
APUNTANDO AL FUTURO

E. J. ARMAZA ARMAZA/E. ATIENZA MACÍAS/M. A. BOLDOVA PASAMAR/I. DE MIGUEL BERIAIN/
A. DUARDO SÁNCHEZ/A. EMALDI CIRIÓN/I. CONAL FUERTES/F. FLORES MENDOZA/
L. F. HERNÁNDEZ GARCÍA/G. LAZCOZ MORATINOS/J. LÓPEZ GOROSTIDI/P. NICOLÁS JIMÉNEZ/
E. PAYÁN ELLACURÍA/A. PERIN/C. M. ROMEO CASABONA/M. A. RUEDA MARTÍN/
E. SOLA RECHE/C. TRINCADO CASTÁN/A. URRUELA MORA/S. I. VERDUGO GUZMÁN

I.	INTRODUCCIÓN	170
	1. Objetivos	170
	2. Hipótesis de partida	171
II.	AMENAZAS COMPLEJAS EN EL CIBERESPACIO, ESTADO DEL ARTE Y PROSPECTIVA.	171
III.	EL MARCO JURÍDICO DE PARTIDA	173
	1. Los derechos fundamentales y libertades públicas.	173
	2. La función del Derecho penal ante la ciberseguridad y los ciberdelitos.	174
IV.	LA INSUFICIENTE INTERVENCIÓN DEL LEGISLADOR PENAL.	175
V.	LAS ESCASAS E INSUFICIENTES REFERENCIAS JURISPRUDENCIALES EN EL ENTORNO DE LOS CIBERDELITOS	177
VI.	LOS DELITOS RELACIONADOS CON EL CIBERESPACIO Y LAS TIC EN EL CÓDIGO PENAL	178
	1. El delito de intrusión en un sistema de información: un objetivo mal resuelto	179
	2. Los delitos de daños contra datos, programas, documentos y sistemas de la información	182
	3. El llamado delito de ciberespionaje y el descubrimiento y revelación de secretos, ¿una cuestión de proporcionalidad?	184
	4. La denegación de servicios, ¿punible en el Derecho español?	188
	5. La suplantación de identidad digital, un fraude de identidad	189
	6. Un fenómeno criminal transversal: la desinformación o la propagación de noticias falsas	190
	7. La sanción penal de algunos actos preparatorios: sus fallos e insuficiencias	192
	8. La necesidad político-criminal de revisar los ciberdelitos cometidos en el ámbito de organizaciones o grupos criminales	193
	9. Posibilidades del Protocolo Adicional al Convenio Europeo sobre Ciberdelincuencia para asegurar la atribución de la jurisdicción penal frente a la deslocalización de los delitos transnacionales.	194
VII.	EN LA FRONTERA DE LOS CIBERDELITOS Y LA IA: LIBERTAD DE EXPRESIÓN, DATOS PERSONALES Y EL BIG DATA	196
VIII.	RESPONSABILIDAD PENAL E INTELIGENCIA ARTIFICIAL	197
	1. Posibilidad dogmática y conveniencia de atribución de responsabilidad penal a los sistemas de IA, a los seres humanos que los diseñan, mantienen o utilizan, o a todos —o varios de— ellos	198

2. La IA como instrumento en la justicia penal	198
3. El futuro marco europeo: la propuesta de Reglamento y su posible impacto en el ámbito del Derecho Penal	200

LOS AUTORES DE LA OBRA

A. MIEMBROS Y PARTICIPANTES EN EL PROYECTO DE INVESTIGACIÓN.	203
B. COAUTORES INVITADOS AJENOS AL PROYECTO	204